4ª edição
IBM Security Forum

Enterprise Security Intelligence

Felipe Peñaranda Silva
CISSP, PCI-QSA, ITIL-Service Manager
IBM-Security Tiger Team - Latin America
felpenar@br.ibm.com

Março, 2011

Agenda

- Perspectiva IBM em Segurança da Informação
- O que é *Enterprise Security Intelligence (ESI) ?*
- Posicionamento IBM em *ESI*

Perspectiva IBM em Segurança da Informação

Um novo mundo de oportunidades …*"A Smarter Planet"*

Globalização e Recursos disponíveis globalmente

Billhões de aparelhos móveis acessando a WEB

Acesso a grandes volumes de informação em tempo real

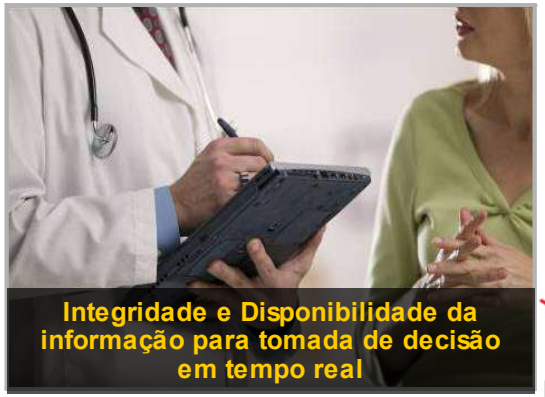
Novas formas de colaboração

Novas Possibilidades

Novas Complexidades

Novos Riscos

A Segurança da Informação nos possibilita endereçar estes riscos e, assim, inovar de maneira confiável …



Desafios em Segurança

Motivadores *chaves* para os projetos de Segurança

Maior Complexidade

Em breve, haverá **1 trilhão** de dispositivos conectados no mundo

Custos crescentes

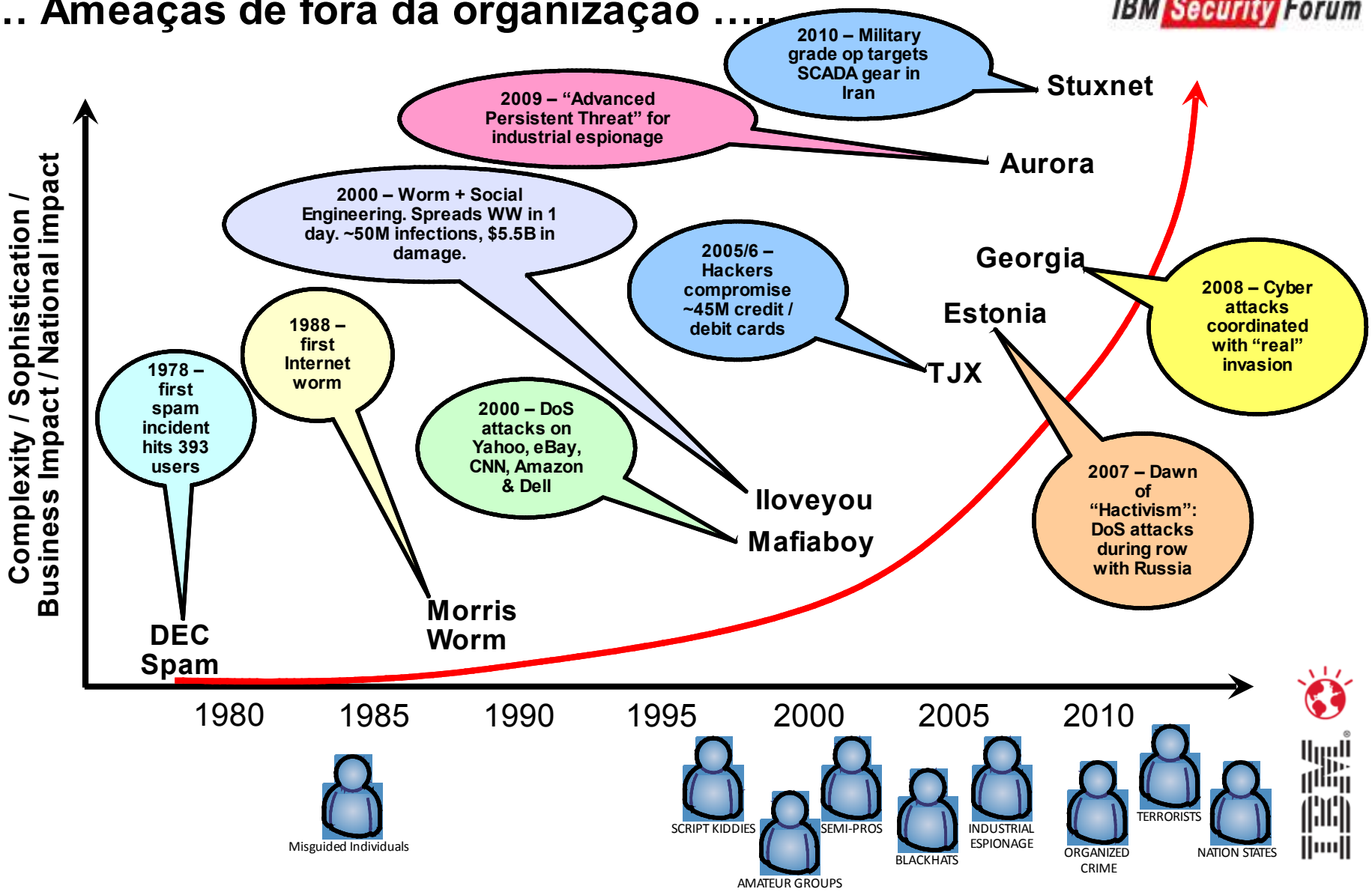
Gastos de empresas americanas em governança, riscos e compliance alcançarão **$29.8 bilhões** em 2011

Compliance

O custo de vazamento de dados chegou a **$204** por registro de cliente comprometido

Source: http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html

… Ameaças de fora da organização ….



…e ameaças de dentro da organização:

4ª edição IBM Security Forum

- **Rogue trading**
  - October 5, 2010: French trader guilty over Société Générale scandal: Jérôme Kerviel jailed after being found guilty of all charges in trading fraud that cost bank €4.9bn

- **Theft of client records and proprietary trading systems**
  - December 11, 2010: Former Goldman Sachs Programmer Sergey Aleynikov convicted for theft of code from the high-frequency trading system that generates millions of dollars in annual profits

- **Theft of celebrity phone records**
  - September 28, 2010: India's Department of Telecommunications amended telecom licensing rules for national and international long-distance operators, to address security concerns on their networks

- **Wiki Leaks**
  - July 30, 2010: A US Army private, Bradley Manning, suspected of leaking classified material, including videos and other documents, has been transferred from Kuwait to a Marine Corps brig in Quantico

O que é *Enterprise Security Intelligence ?*

Por que ESI ?

Modelo de Maturidade - Segurança da Informação																			
Perímetro				Infraestrutura				Gestão de Identidades e Acessos				Segurança na Aplicação				Database Security			
Nível I				Nível II				Nível III				Nível IV				Nível V			
FIREWALL-VPN	ANTIVIRUS	NETWORK-IPS	ANTI-SPAM	VULNERABILITY-MGMT	PATCH-MGMT	HIPS	ENDPOINT PROTECTION	USER PROVISION-INGS	ENTERPRISE SSO	WEB ACCESS MGMT	SIEM	DAST	WEB SERVICES SEC	SAST	ENTITLEMENT MGMT	DB VULNERABILITY	DAM	DATA MASKING	DLP

Definição de *intelligence*

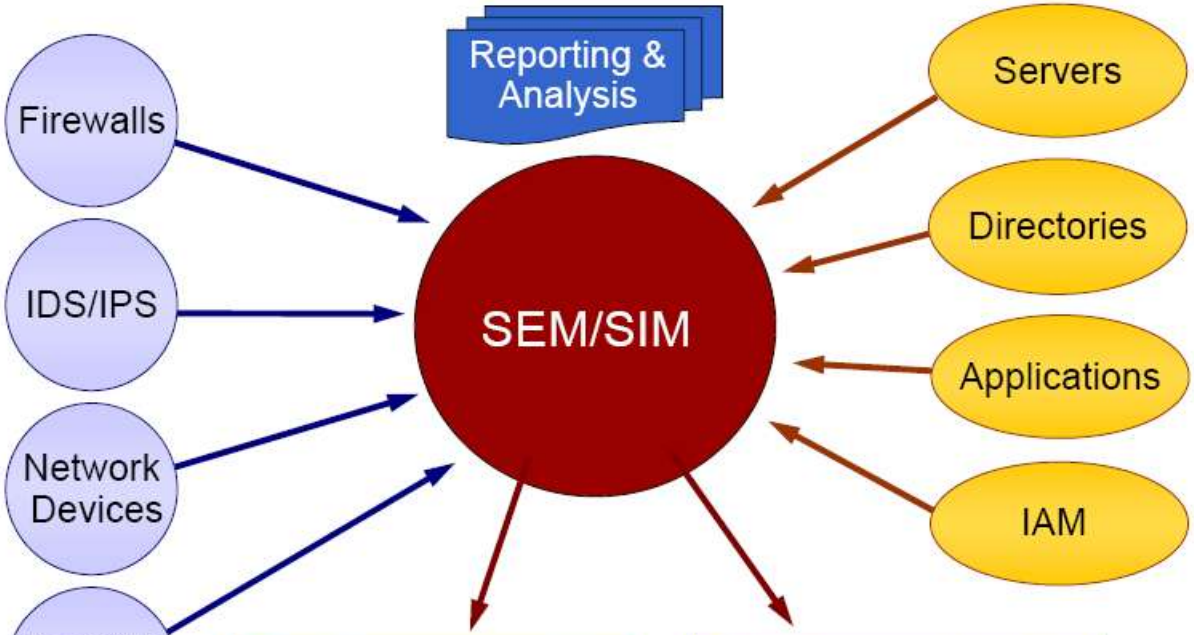
Intelligence

- **The collection of information**

- **The ability to acquire and apply knowledge and skills**

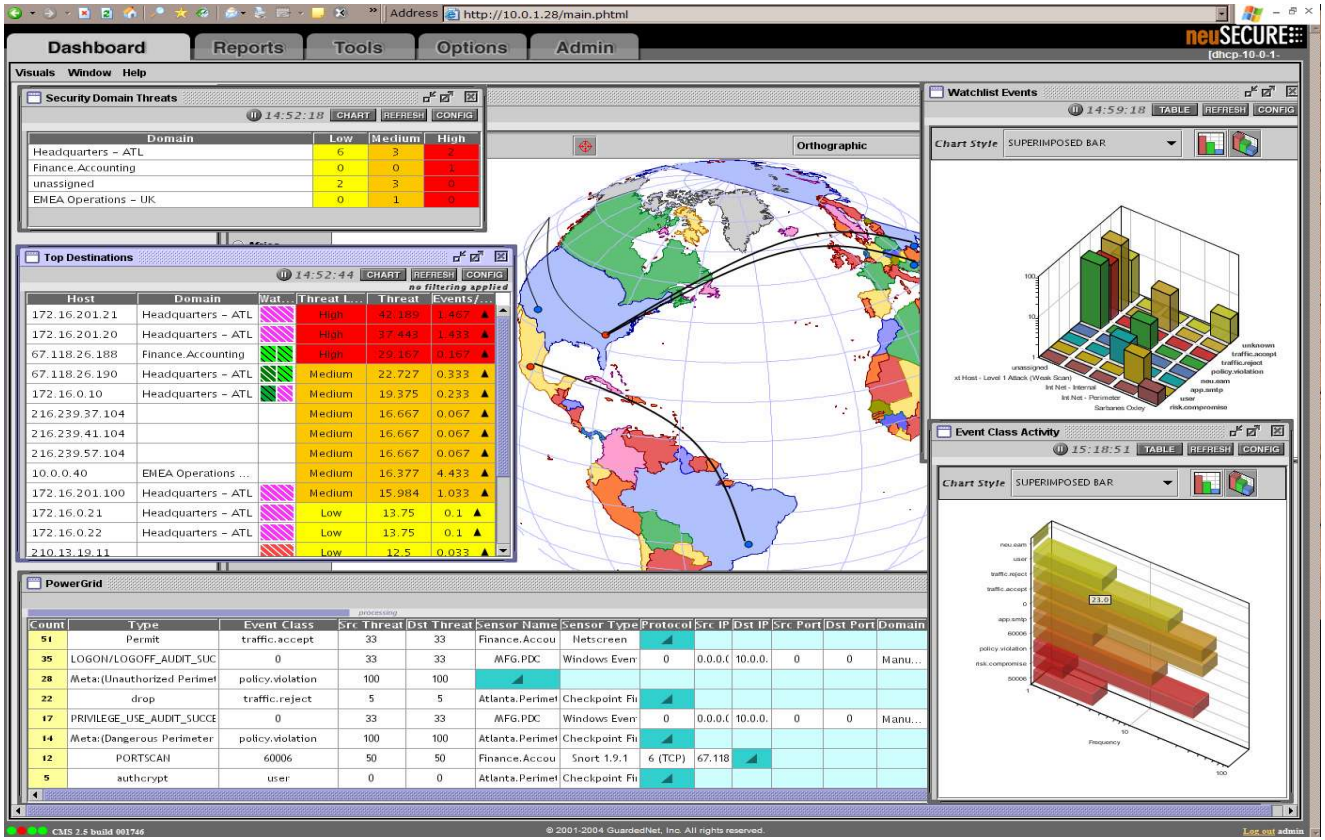
The new Oxford American Dictionary

Security Information and Event Management Defined

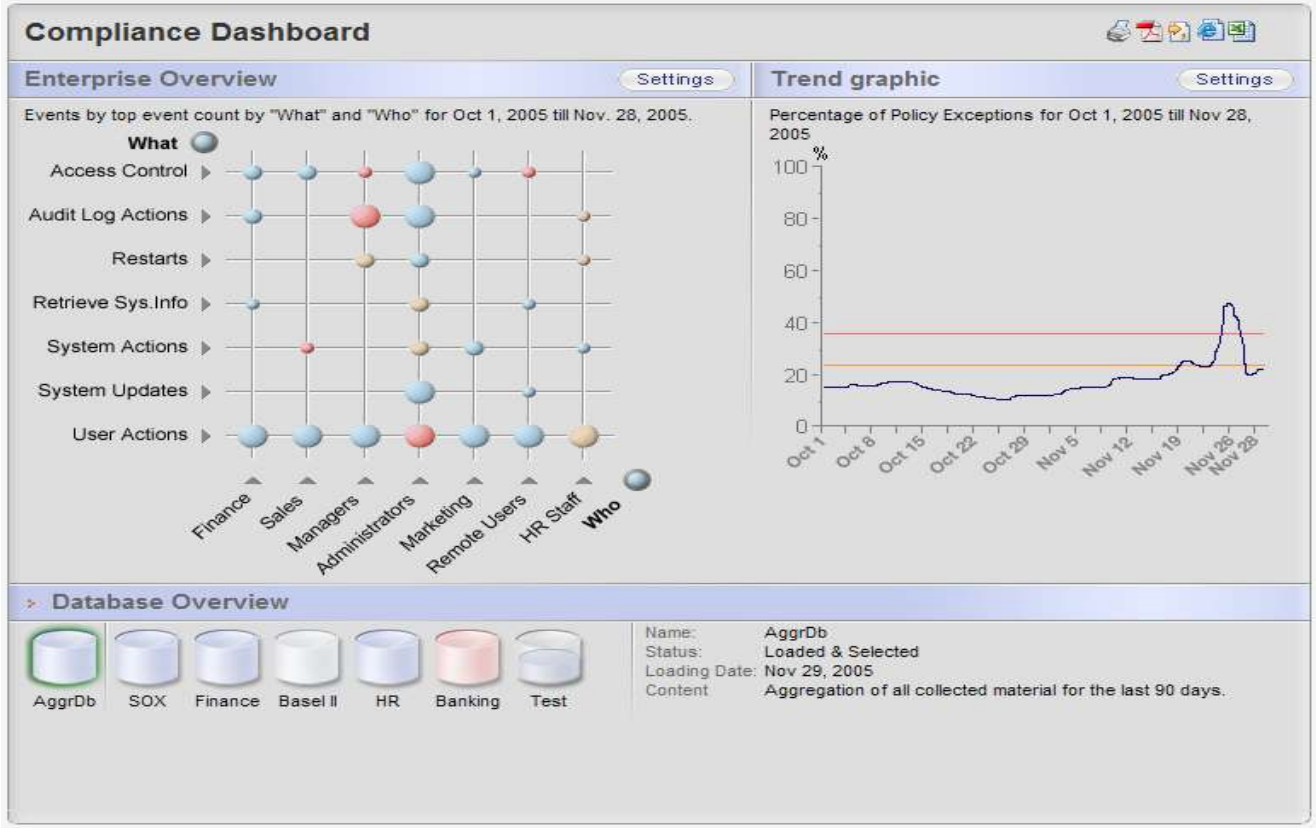


Gartner

SEM Indicators (Security Event Management)

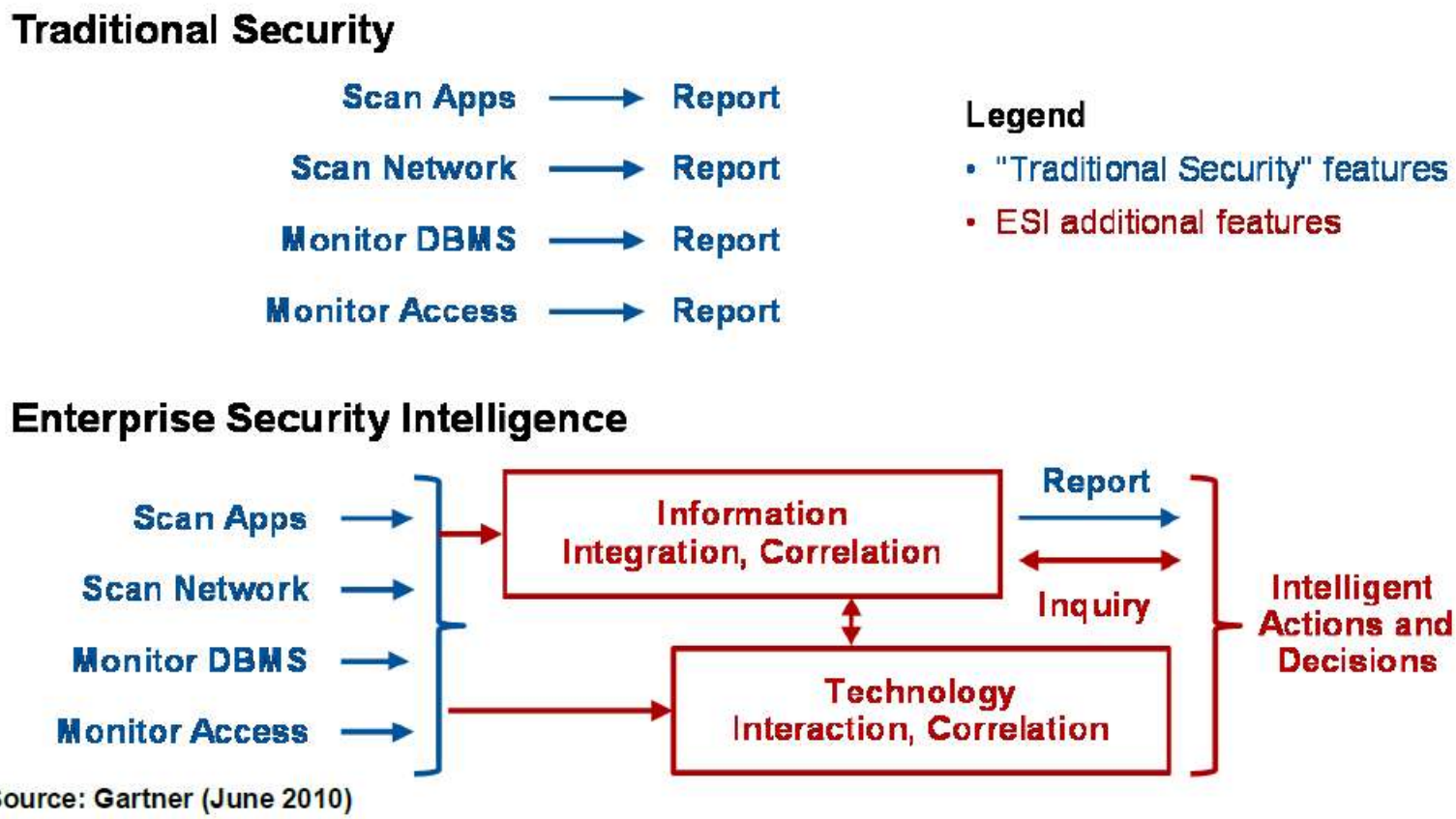


SIM Indicators (Security Information Management)



The ESI concept includes all the capabilities of traditional enterprise security. Scanners and monitors will continue to detect vulnerabilities (see Figure 1).

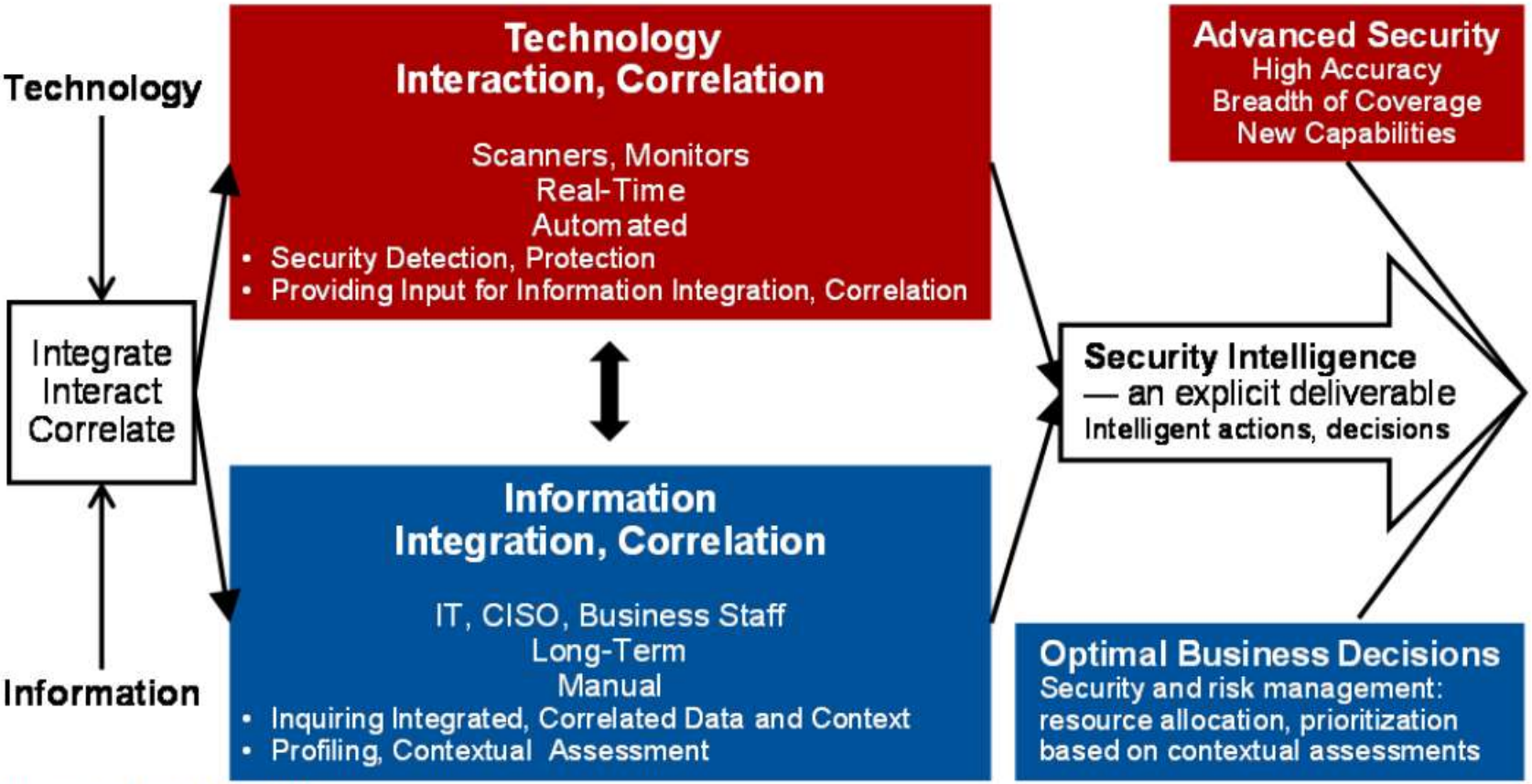
Figure 1. Traditional Security Versus Enterprise Security Intelligence



Source: Gartner (June 2010)

However, ESI explicitly introduces two new critical elements:

Figure 2. ESI Essentials



Source: Gartner (June 2010)

O que é ESI ?

- ***"Technology interaction and correlation:*** *These are typically automated actions that primarily perform (quasi-) real-time interaction and correlation between different security software and hardware, between different scanners and monitors (for example, [quasi-] real-time inputting of the results of one type of a scan into another to more accurately detect vulnerabilities, or dynamic masking of sensitive data discovered by static masking)."*

Source: Gartner, 2010

O que é ESI ?

- *"**Information integration and correlation:** The information that scanners and monitors discover will be integrated in a repository that will store and retain information received from static and dynamic feeders; from information collected in different phases of the software life cycle (for example, programming, testing and operation); from different network layers (for example, data transport, presentation and application); and from IAM, network, database and application monitors. This information will be available for correlation, interrogation and analytics."*

Source: Gartner, 2010

Exemplos de interação entre tecnologias de Segurança

- SAST e DAST
- WAF e DAST
- Data Masking, DAM e IAM
- SIEM e IAM (IAI)

Integração e Correlação de informações de Segurança

- Repositórios
  - *Security Information (SIEM)*
  - Informação de Contexto (business, compliance, riscos, ...)
- *Profiles*
  - Enterprise Asset Profile (IT-GRCM)
- *Policy Engines*
  - *Policy Enforcement*
  - Priorização de Ações

O que se espera como resultado do ESI

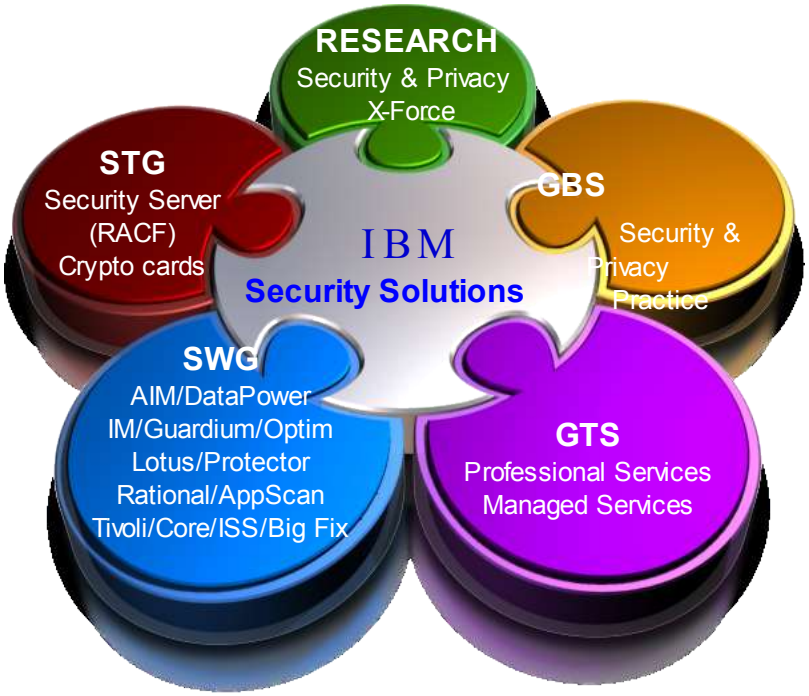
- *Queries* substituindo *scans*
- *Queries* multidimensionais ao invés de relatórios lineares
- Integração de informações de segurança e contexto de negócio
- *Advanced Security*
- Otimização nas decisões de negócio

Posicionamento IBM em *ESI (Enterprise Security Intelligence)*

Histórico IBM em Segurança da Informação (aquisições)

DASCOM

watchfire



OUNCE LABS an IBM company

access360 A Better Way To Manage Access Rights

Guardium SAFEGUARDING DATABASES™ | AN IBM® COMPANY

DATAPOWER

princeton softech an IBM® Company

consul an IBM company

BIGFIX An IBM Company

INTERNET SECURITY SYSTEMS™

OPENPAGES Clarity. Confidence. Control.

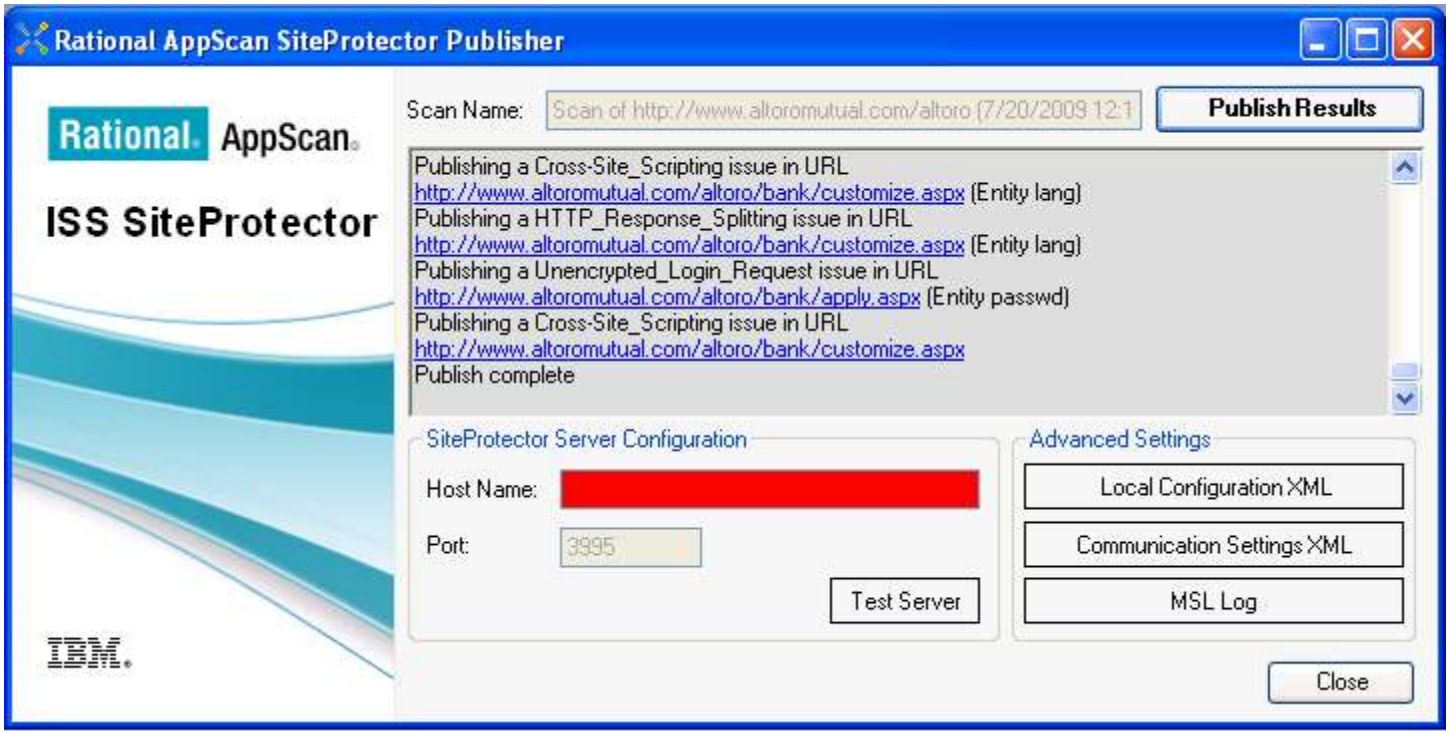
ENCENTUATE An IBM Company

IBM em ESI

- Integração de tecnologias
- Integração de informações

Integração de Tecnologias

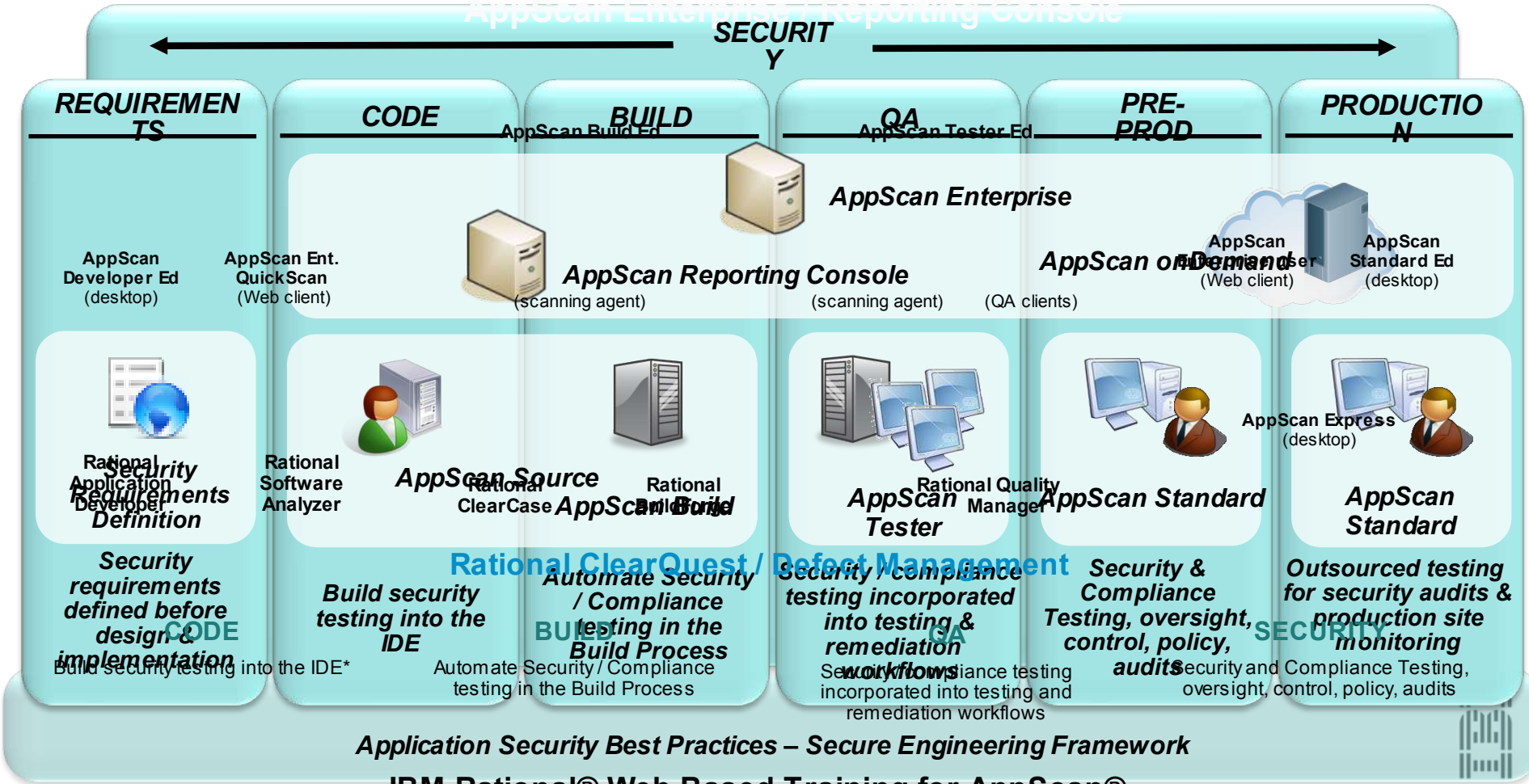
Integração de tecnologias: WAF e DAST



The extension will display the publishing results during the upload. Close the extension when the publishing is complete

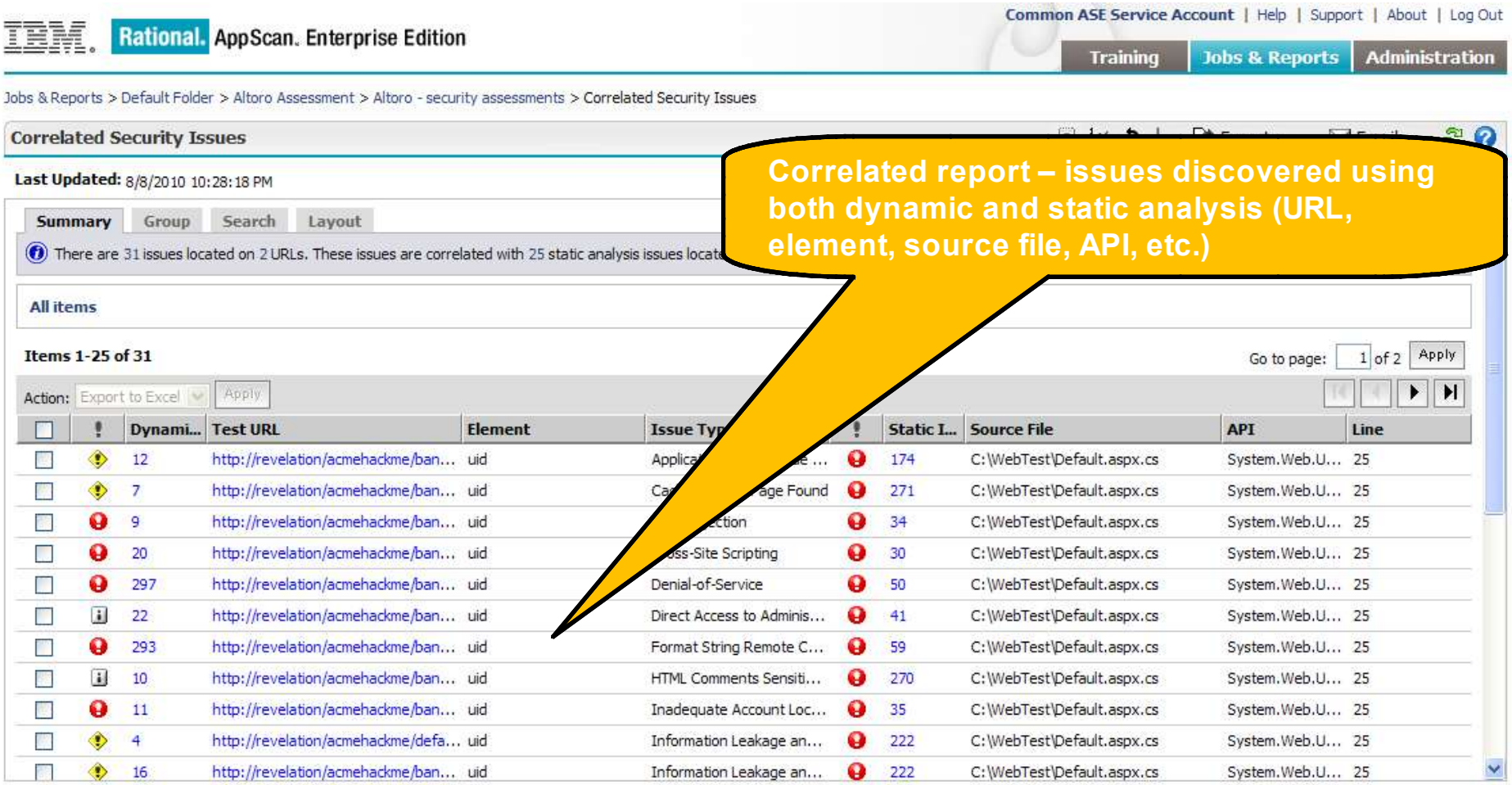
Integração de Tecnologias: SAST e DAST

Rational AppScan diagram.png



IBM Rational® Web Based Training for AppScan®

Integração de Tecnologias: SAST e DAST



Integração de Tecnologias: Data Masking, DAM e IAM

Médicos precisam ver informações sobre sintomas mas não informações pessoais

Paciente: *Maria José*
CPF: [CPF]
Tel: [Tel]

...: Sinais associados e sintomas incluem dores, febre...

Visão do médico

CPF & tel. Não são bloqueados – Área financeira precisa ver isso,mas não os sintomas

Patient: *Maria José*
CPF: *517.123.456-10*
Tel: *031-3343-1189*

...: Sinais associados e sintomas incluem

[sintomas]
...

Visão da área financeira

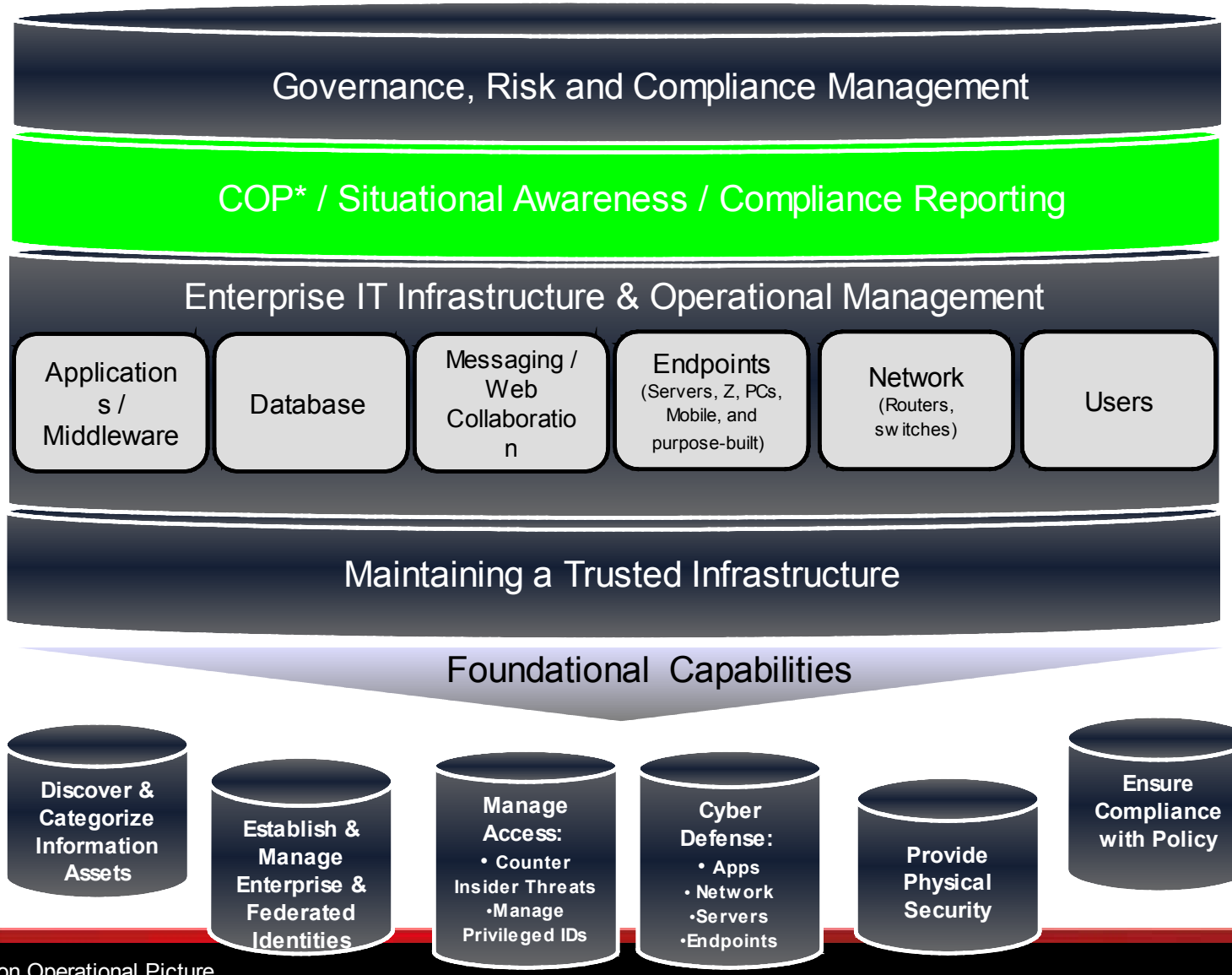
Integração de Tecnologias: IAM e SIEM (IAI)

Tivoli-IAM

Tivoli- SIEM

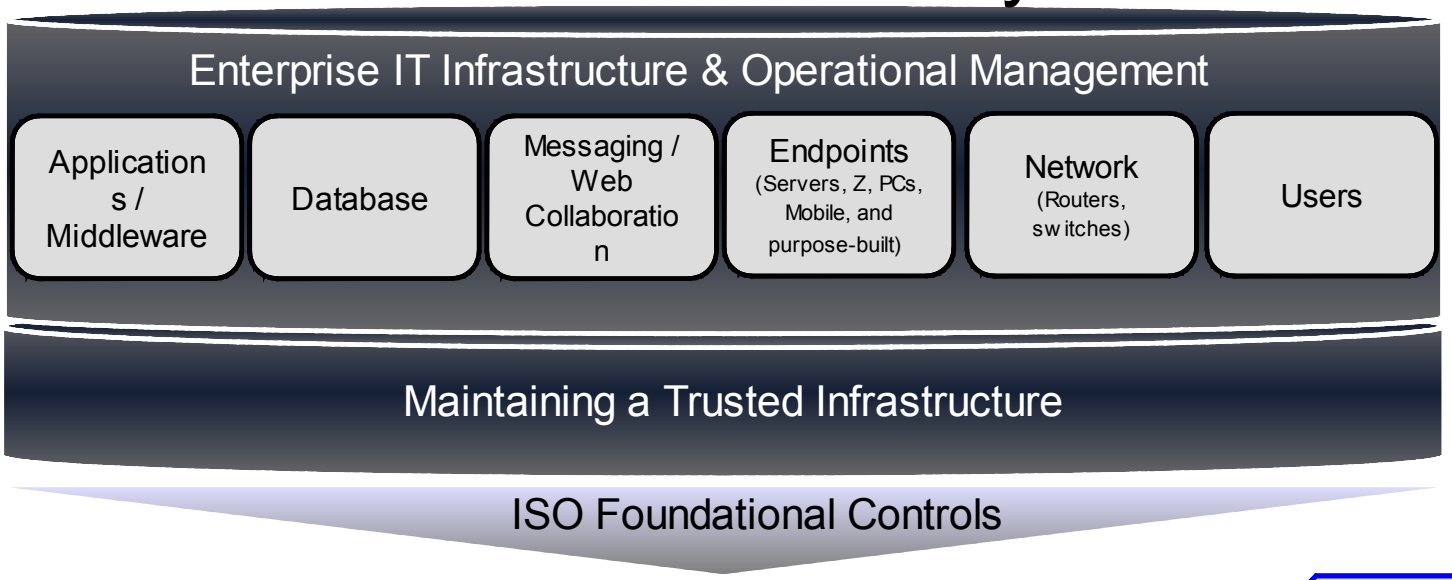
Integração de Informações

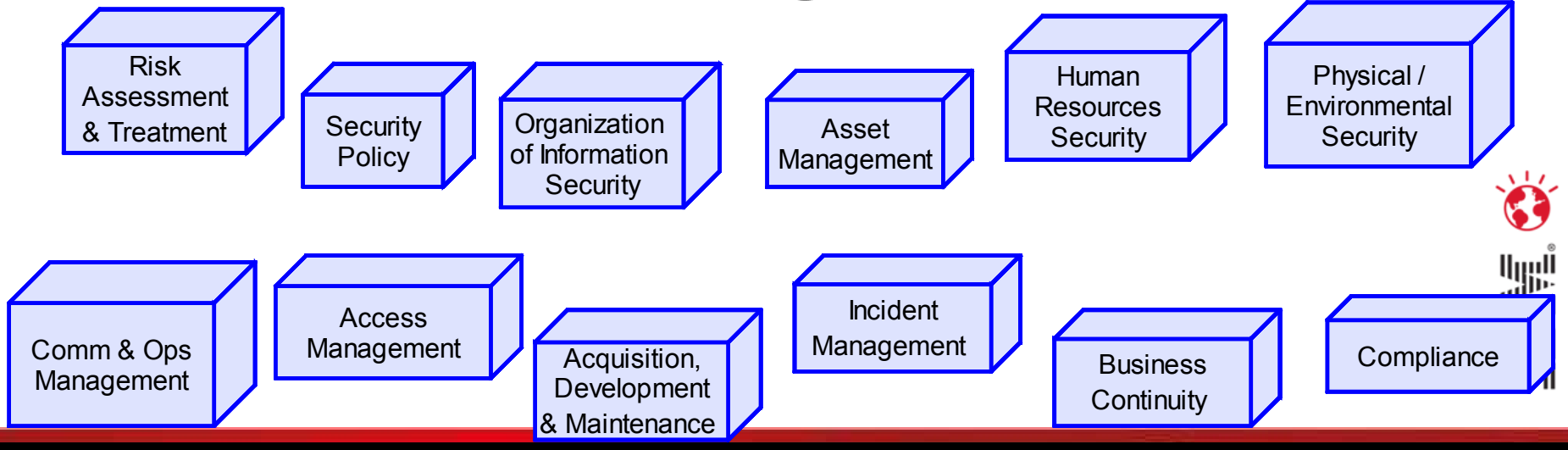
Cybersecurity in Depth: Required Capabilities



* Common Operational Picture

Another View: Standards Based Maturity Models





The future (closer than you may think): automating security & resilience

4ª edição IBM Security Forum

Advanced Analytics:

- autonomic attack pattern recognition
- machine and network speed
- deep packet inspection
- enables "intuitive situational awareness"

Governance, Risk and Compliance Management

Composite COP (Multi-Environment)

Enterprise IT Infrastructure & Operational Management

- Applications / Middleware
- Database
- Messaging / Web Collaboration
- Endpoints (Servers, Z, PCs, Mobile, and purpose-built)
- Network (Routers, switches)
- Users

Maintaining a Trusted Infrastructure

Sense & Respond Cyber Defense:

- acts on intelligence from advanced analytics
- Enables automatic re-configuration & re-provisioning

Foundational Capabilities

- **Discover & Categorize Information Assets**
- **Establish & Manage Enterprise & Federated Identities**
- **Manage Access:** • Counter Insider Threats •Manage Privileged IDs
- **Cyber Defense:** • Apps • Network •Servers •Endpoints
- **Provide Physical Security**
- **Ensure Compliance with Policy**

MOCA Purpose – *Address Hard engineering problems for cloud and cyber defense*

- MOCA = Mission Oriented Cloud Architecture
  - –Network awareness
  - –**Situational awareness**
  - –Application and database vulnerability detection
  - –Network defense
  - –Cloud management

- Why MOCA? Three reasons:
  - –Develop leap ahead technologies
  - –Work down customer hard engineering problems
  - –Demo technology innovations

Press room
Press releases
Press kits
Photo gallery
Biographies
Background
Press room feeds
Global press resources
Press room search
Media contacts

Related links
- IT Analyst support center
- Investor relations

U.S. Air Force Selects IBM to Design and Demonstrate Mission-Oriented Cloud Architecture for Cyber Security

Cloud model will introduce advanced cyber security and analytics technologies capable of protecting sensitive national data

Press release
Contact(s) information
Related XML feeds

ARMONK, N.Y. - 04 Feb 2010: The U.S. Air Force has awarded IBM (NYSE:IBM) a contract to design and demonstrate a secure cloud computing infrastructure capable of supporting defense and intelligence networks. The ten-month project will introduce advanced cyber security and analytics technologies developed by IBM Research into the cloud architecture.

The project will push the technology boundaries of cloud computing with an infrastructure design that not only supports large-scale networks, but meets rigorous security standards and the government's Information Assurance guidelines for all networks. The Air Force's network manages the operations of nine major commands, nearly 100 bases, and 700,000 active military personnel around the world.

"Our goal is to demonstrate how cloud computing can be a tool to enable our Air Force to manage, monitor and secure the information flowing through our network," said Lieutenant General William Lord, Chief Information Officer and Chief, Warfighting Integration, for the U.S. Air Force. "We examined the expertise of IBM's commercial performance in cloud computing and asked them to develop an architecture that could lead to improved performance within the Air Force environment to improve all operational, analytical and security capabilities."

IBM researchers, software architects, analytics specialists and cyber security experts will work with military personnel and other federal agencies to demonstrate an unprecedented level of security and network resiliency into the Air Force cloud design. Advanced "stream computing" analytics will be a key design component. This technology, coupled with sensors, monitors and other detection devices, would enable the Air Force to perpetually analyze the massive amounts of data flowing through its network and get fast, accurate, and actionable insights about possible threats, such as cyber attacks and network, system or application failures, while automatically preventing disruptions.

Contact us
→ Contact a media relations representative
→ Site feedback

Share
Facebook
Twitter
LinkedIn

Document options
E-mail this page

Press kits
→ IBM Business Analytics and Optimization
→ IBM Cloud computing
→ IOD EMEA 2010

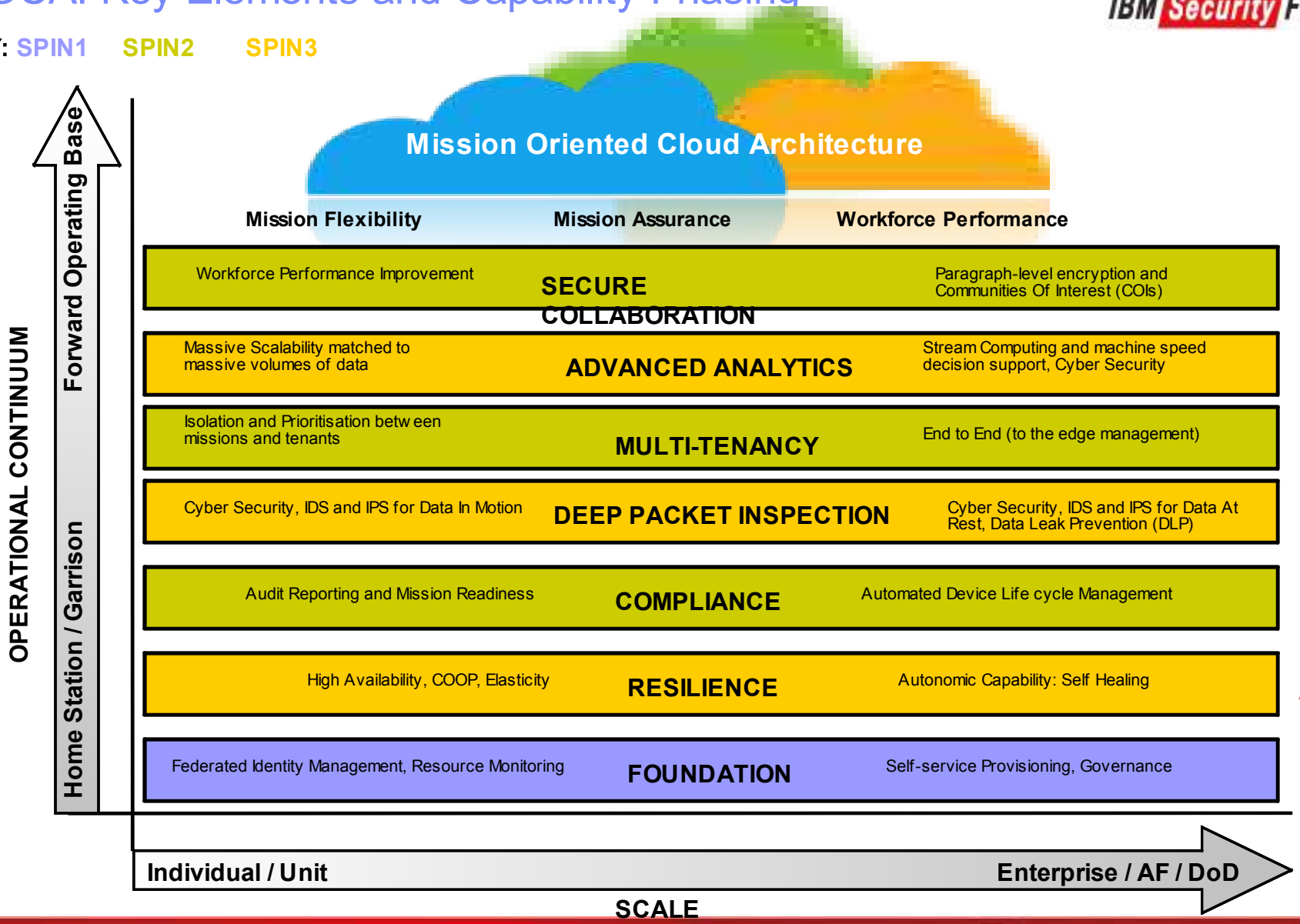
IBM Press Room Twitter

Who from IBM is working on MOCA?

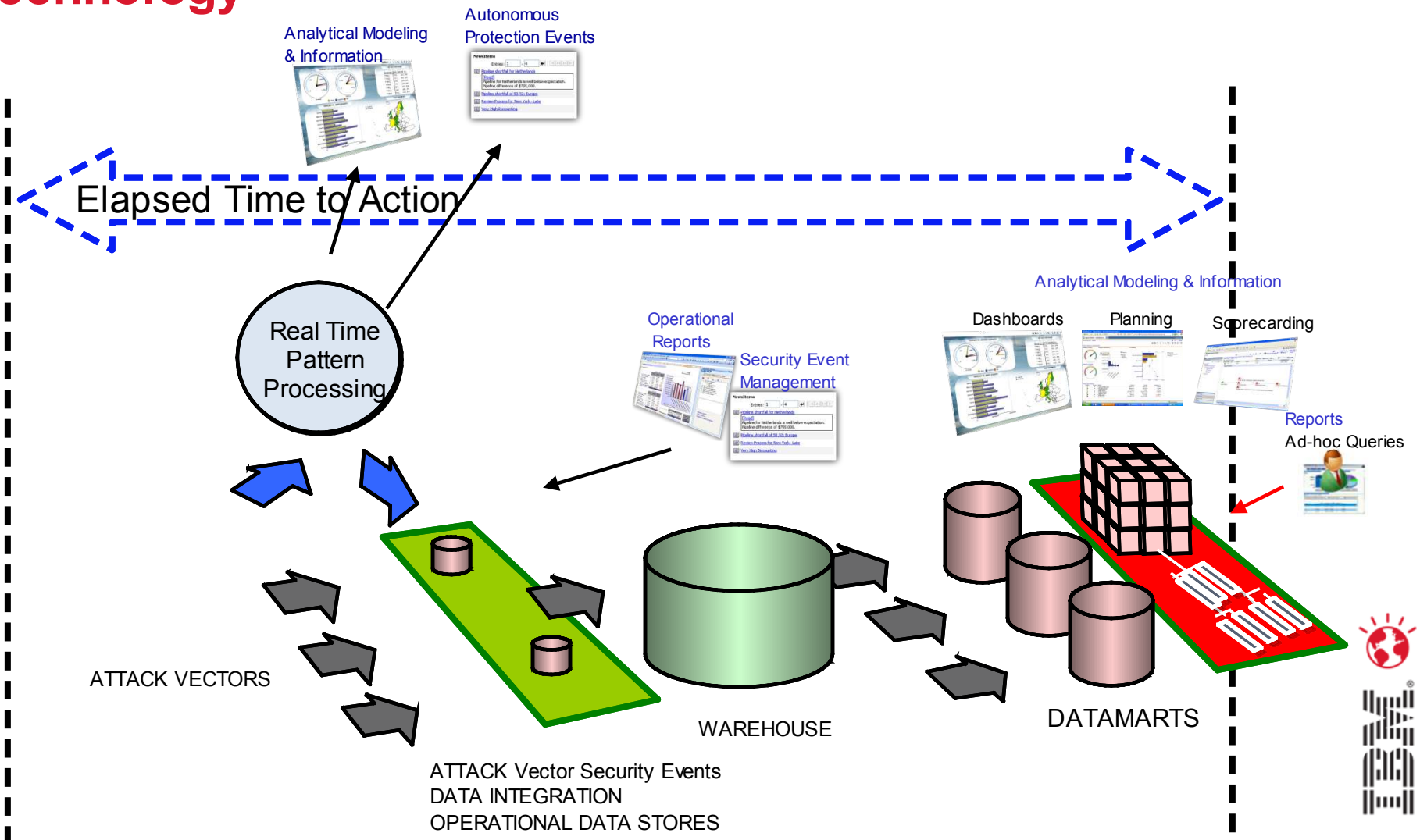
- IBM Research
- IBM Security
- Cloud Engagements Group
- CTO Office, US Federal
- GBS Federal
- Analytic Computing Group
- IBM Institute for Advanced Security
- Systems and Technology Group
- IBM Partners & whoever else we need…….

MOCA: Key Elements and Capability Phasing

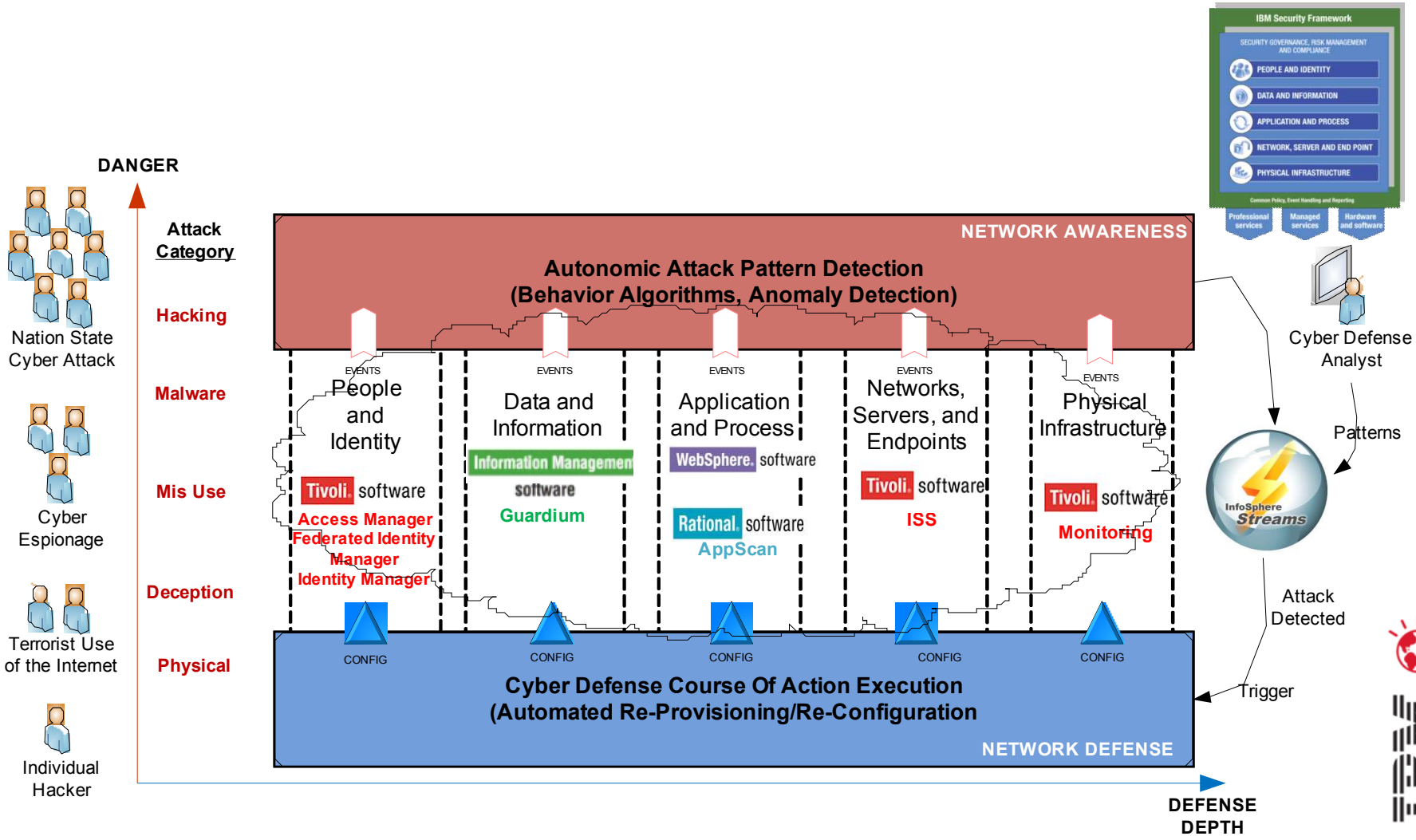
KEY: SPIN1 SPIN2 SPIN3



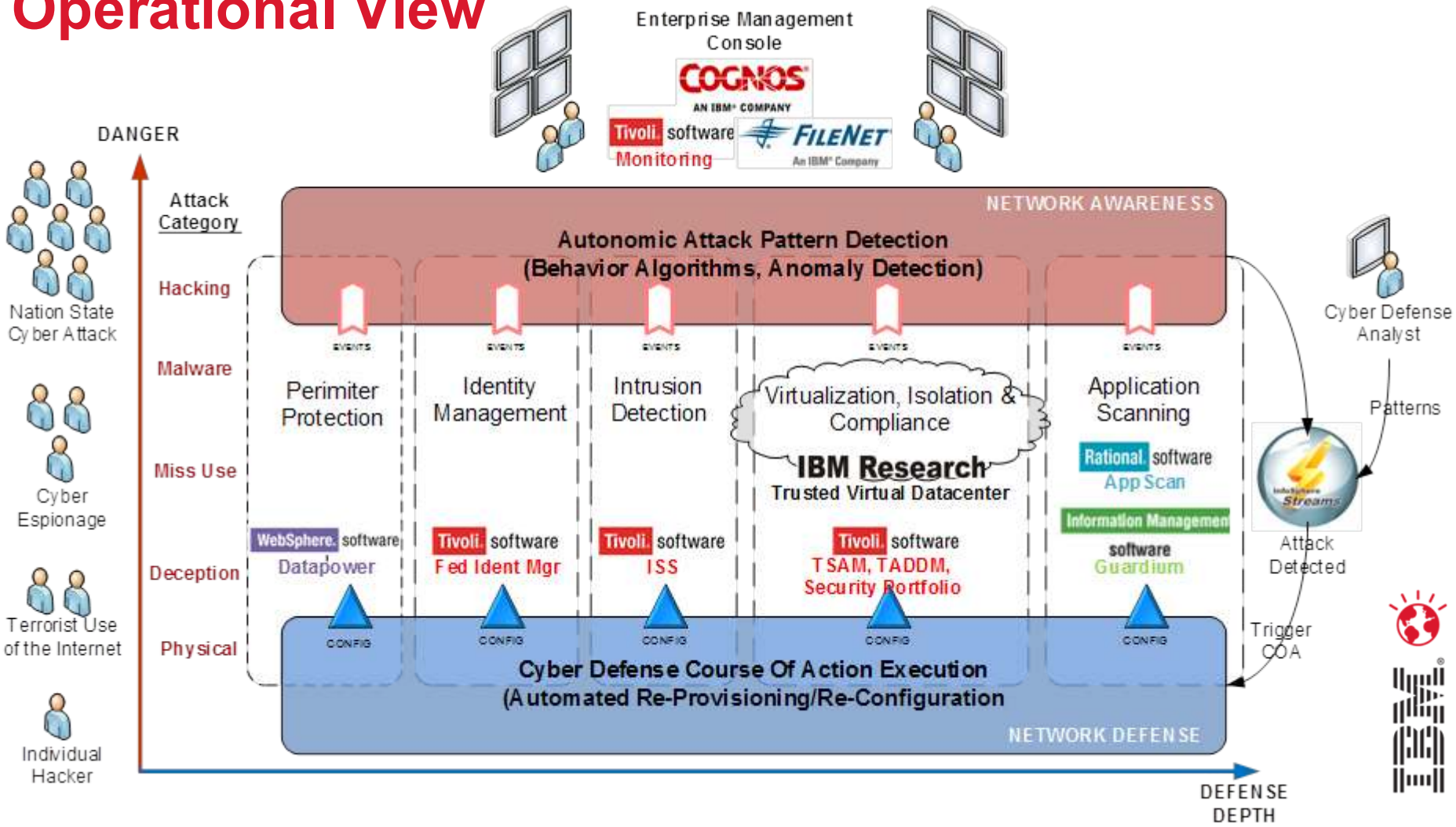
Pattern Recognition in Real Time – A Streams Technology



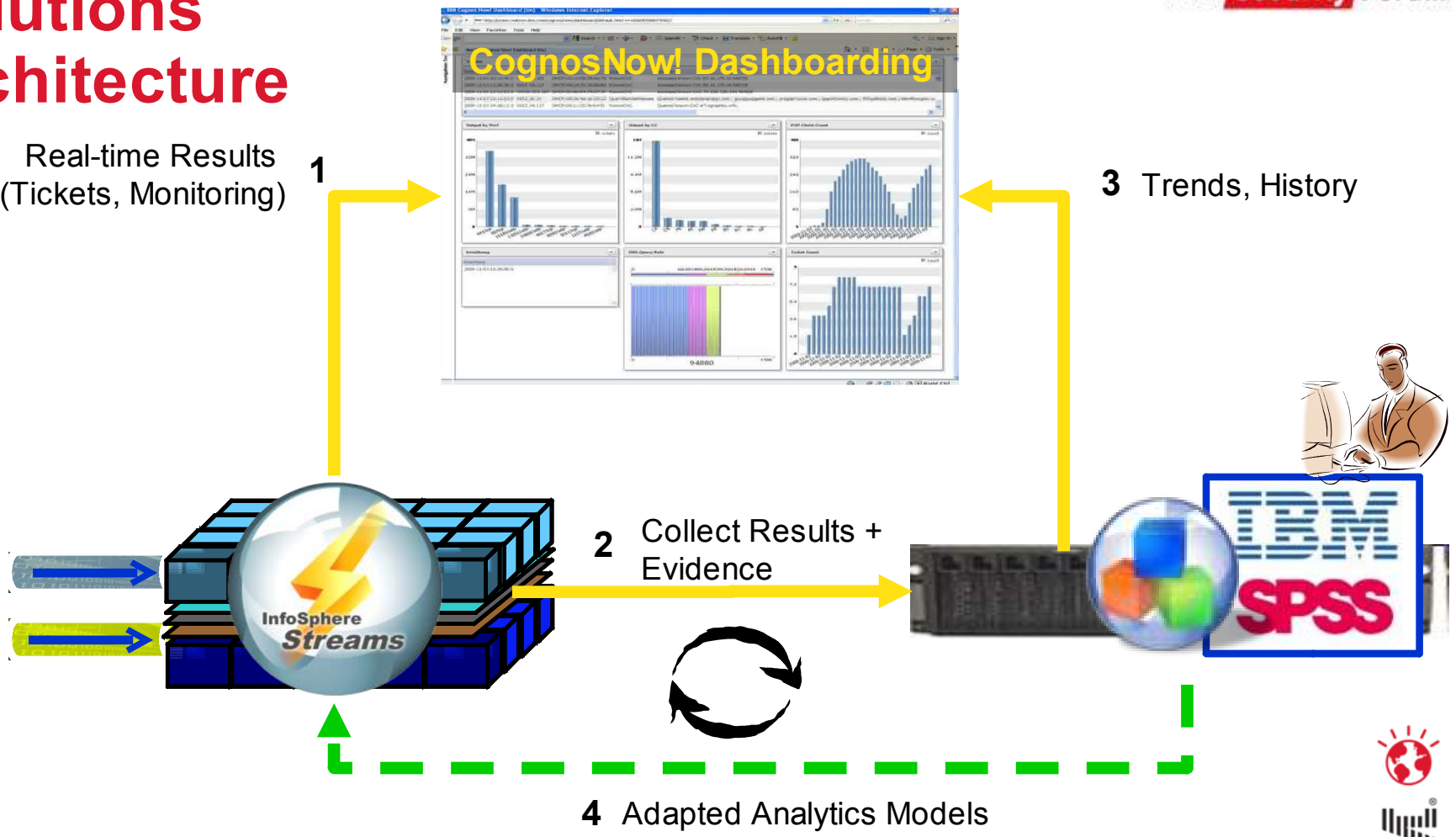
IBM's Security Methodology



(MOCA) Mission Oriented Cloud Architecture – Operational View



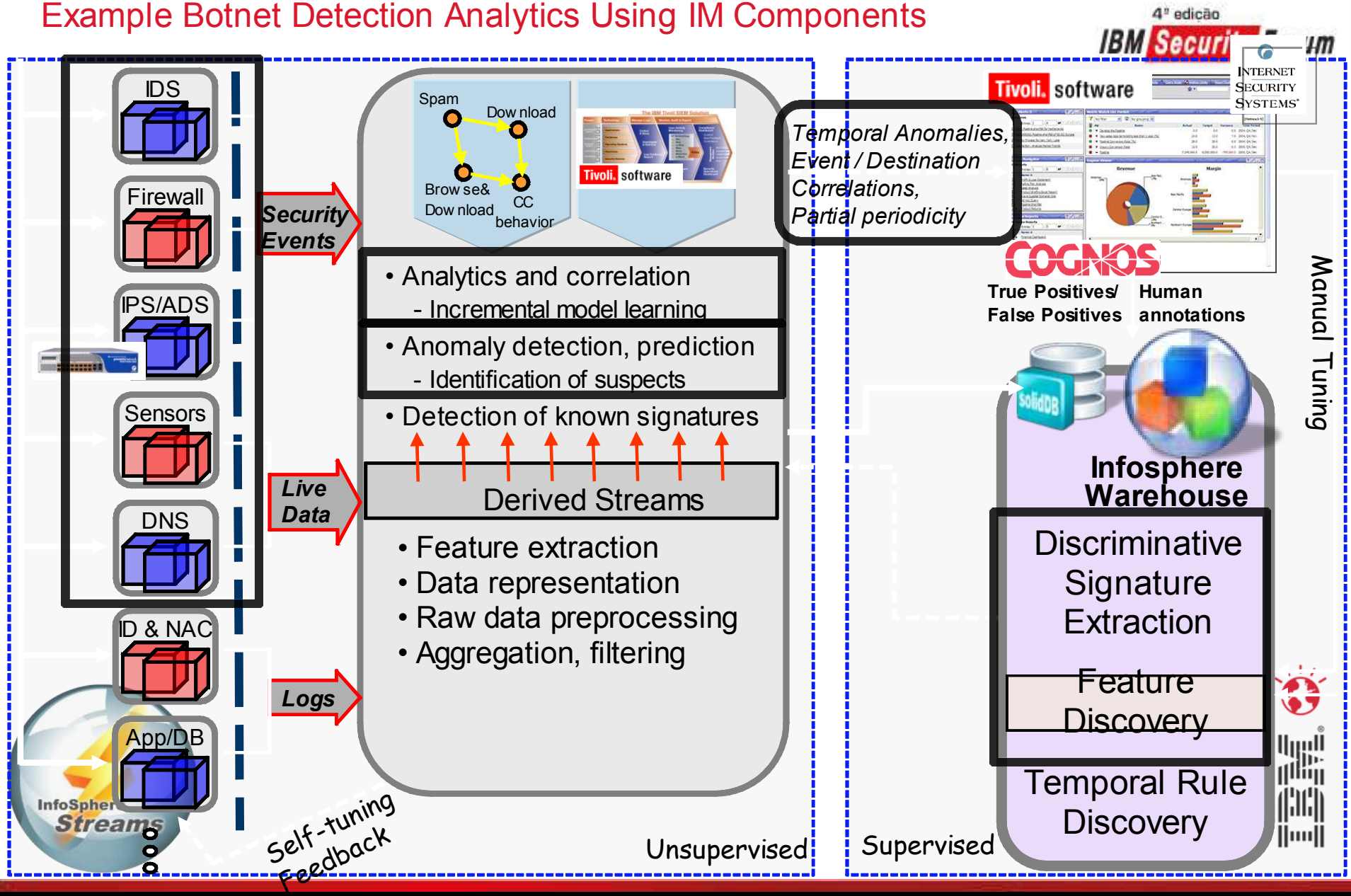
Solutions Architecture



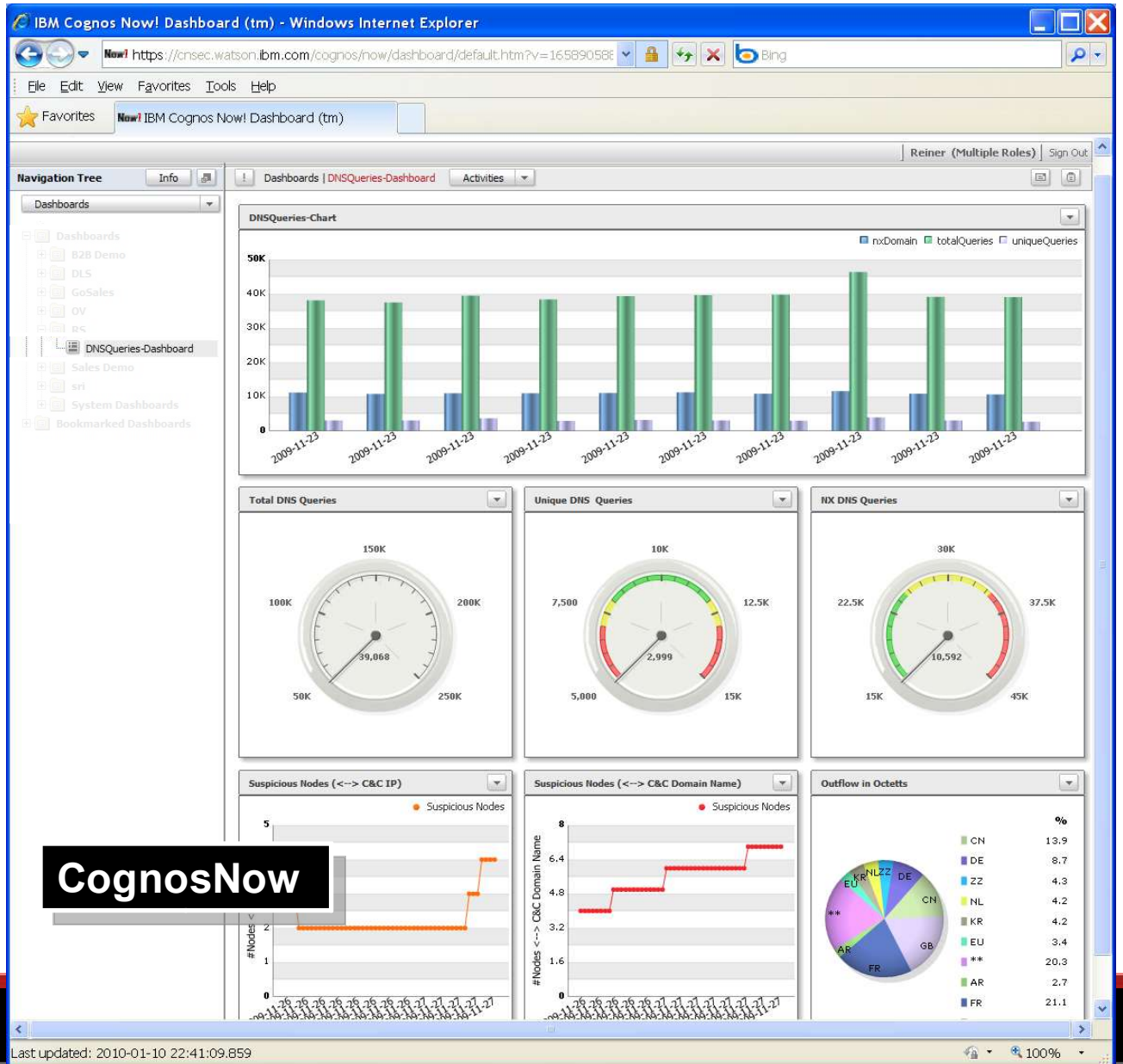
Unsupervised Real-Time Analytics

Supervised Learning

Example Botnet Detection Analytics Using IM Components



Predictive Analysis Dashboard Configuration



CognosNow

Analytics driven security intelligence

Moderators: Raj Nagaratnam, CTO IBM Security Solutions , Marc van Zadelhoff, Dir Security Solutions Strategy
Subject Matter Experts: Koos Lodewijkx, IBM Security Strategy Lead
Board Member Participant: Tony Spinelli, Equifax, SVP, Chief Security & Compliance Officer

Abstract

While the high degree of interconnectivity enabled by the Internet has been a driver for the digital economy, easy accessibility to key enterprise, government, industrial and academic institutions to friend and foe alike and the absence of adequate, consistent safeguards and security controls has greatly increased the level of risk to national economic and defense interests, and enterprise assets. While enterprises and institutions use variety of tools (e.g., intrusion prevention systems, identity and access management systems) to get a better handle on their security posture, the need exists for technologies and processes to gain timely insight based on ongoing events and relevant data to make informed decisions to defend against threats.

This session will facilitate an interactive discussion to understand the emerging threats and risks clients want to handle by gaining insight of ongoing events and available business information. We will share an approach to gain insight on threats and risks at real time, supported by a demonstration a risk dashboard, using analytics technologies, that provide visibility to threats and risks through analytical insight to make timely decisions, and control and automation approaches to take timely action. IBM looks forward to solicit feedback to shape our strategy towards gaining threat and security intelligence.

Enterprise Security Intelligence

Felipe Peñaranda Silva
CISSP, PCI-QSA, ITIL-Service Manager
IBM-Security Tiger Team - Latin America
felpenar@br.ibm.com